The ArtsXchange

Part of the T4 Trust

E-Safety Policy

Version Control:

Action	Name	Date
Prepared by	Jan Tomlinson	February 2022
Approved by	Board of Governors	February 2022
Revised by	Adelle Miles	May 2022
Revised by	Jan Tomlinson	September 2022
Approved by	Board of Governors	September 2023
Revised by	Adelle Miles	August 2023
Reviewed by	Gosia Klosek	September 2023
Approved by	Board of Governors	15 September 2023

Table of Contents

Key Contacts - The ArtsXchange

Head of College: Gosia Klosek
Contact details: 020 4568 4747
Email: gosia.klosek@theartsxchange.com
Assistant Head Teacher and Designated Teacher for Looked After Children: Darien Delmede-Crawford
Contact details: 020 7527 8102
Email: Darien.Delmede-Crawford@theartsxchange.com
Assistant Head Teacher and Special Educational Needs Co-ordinator: Mihaela Chowdhury
Contact details: 020 7527 8102
Email: Mihaela.Chowdhury@theartsxchange.com,
Lead Welfare Practitioner and Designated Safeguarding Lead (DSL): Adelle Miles
Contact details: 020 4568 4747
Email: Adelle.miles@theartsxchange.com
Deputy Designated Safeguarding Lead (DSL): Gosia Klosek
Email: gosia.klosek@theartsxchange.com
Operational Safeguarding T4 Trust Lead: Lisa Tharpe
Contact details: 020 4568 4747
Email: Lisa.Tharpe@theartsxchange.com
Nominated Governor for Safeguarding and child protection: Justin Warren
Email: Justin.Warren@theartsxchange.com
Child Protection Lead Officer and Local Authority Designated Officer (LADO) Camden: Jacqueline Fearon
Contact details: 0207 974 4556
Email: LADO@camden.gov.uk
Child Protection Lead Officer and (LADO) Islington: Timur Djavit
Contact details: 020 7527 8102
Email: LADO@islington.gov.uk
Virtual School Head for Care Experienced Children & Young People Islington: Matthew Blood
Contact details: 020 7527 3992
Email: matthew.blood@islington.gov.uk
Islington Children Social Care: Multi Agency Safeguarding Hub
Contact details: 020 7527 7400
Email: csctreferrals@islington.gov.uk
Police Referrals: Child Abuse investigation Team (CAIT)
Contact Details: 020 8733 6495 or 020 8733 6500
For emergencies: Call 999
Operation Encompass: Supporting child who are experiencing Domestic Violence
Contact Details: 0204 513 9990
Email: info@operationencompass.org

Prevent: Referrals	Educational Prevent Lead
Contact details: 020 7974 2010	07825 098235
Email: prevent@camden.gov.uk	saira.kamaly@islington.gov.uk

1. Aims

The ArtsXchange aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy is to be read in conjunction with all other policies for The ArtsXchange College with particular emphasis on the need to understand the Safeguarding Policy, Behaviour and Anti-Bullying Policy and Staff Code of Conduct. With safeguarding procedures detailed, including raising and reporting concerns for young people and staff. Please also see the Home Guide on how to use Microsoft Teams and internet safety advice.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for college's on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Including following legislation:

- Serious Crime Act 2015
- The Equality Act 2010
- Education and Inspection Act 2006
- Communications Act 2003
- Sexual Offences Act 2003
- Regulation of Investigatory Power Act 2000
- Data Protection Act 1998
- Malicious Communication Act 1988
- The Human Rights Act 1998
- The Computer Misuse Act 1990

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Head of College to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this Policy
- Agree and adhere to the terms on acceptable use of the college's ICT systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Head of College

The Head of College is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the college whom is also the Deputy Designated Safeguarding Lead. The Head of College will ensure the Governing Board are informed of Online Safety practices and raise areas of further support, developments, or concern.

The Head of College works alongside the IT Team and DSL to ensure online safety and security is monitored and the necessary support and actions are taken to ensure the duty is being fulfilled.

3.3 The Designated Safeguarding Lead

Details of the college's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

In relation to the KCSiE 2023 update, there is emphasis on filtering and monitoring systems and standards, there is added clarification that the Designated Safeguarding Lead has chief responsibility for this within their college.

Governing bodies and proprietors have also been specified as responsible members for ensuring "all staff undergo safeguarding and child protection training" which includes the new outlines of filtering and monitoring systems. This training should be regularly updated, as in line with KCSIE 2023.

The DSL takes lead responsibility for online safety in college, in particular:

- Supporting the Head of College in ensuring that staff understand this policy and that it is being implemented consistently throughout the college
- Working with the Head of College, ICT staff and consultants and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the college child protection policy
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the college behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the Head of College and/or governing board

This list is not intended to be exhaustive.

Staff training to include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring at induction and at regular intervals.

The College Leadership Team and relevant staff should have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when they are identified and in particular those who are potentially at greater risk of harm.

Safeguarding and tech teams should work together to ensure measures are in place and action is taken along with online safety auditing annually.

3.4 The ICT consultants (N S Optimum) and ICT technician

The ICT consultants and ICT technician are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess

effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material

- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the college's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college Behaviour Policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the college's ICT systems and the internet (appendix 3), and ensuring that students follow the college's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of College of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the college's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent fact sheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the college's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All school's/college's have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary education, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating parents/carers about online safety

The college will raise awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during "parents' evenings".

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of College and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of College.

6. Cyber Security

Digital technologies offer young people abundant opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages. The use of digital technologies is now so prevalent and important in society, that we must support young people to have access and reap the benefits of this.

For students with SEND needs, the value of utilising mobile devices and the internet can be even greater than for their non-disabled peers due to things such as the use of assistive technologies to aid and communication and social networking to help students with SEND needs who are isolated to connect to others. Therefore, as professionals working with students with SEND needs, we must be proactive in seeking these opportunities and helping young people we work with to benefit from them.

Due to the rapid advancement of digital technologies young people embrace and understand advancement on the internet and mobile telephones as the 'norm', and view this 'virtual world' as an extension to their physical world. However, this can create some risk to young people that we must be aware of, and as far as possible help young people to understand. Some of the dangers the virtual world can pose to students include:

- Students' attendance and attainment at college can be affected by 'vamping'- lack of sleep due to using technology.
- Students have been 'groomed' online by others (often pretending to be other young people) with the ultimate aim of exploiting them sexually.
- Students have been bullied or 'trolled' by other young people via social networking sites, websites, instant messaging and text messages; this is often known as 'cyber-bullying'.
- Inappropriate (i.e., threatening or indecent) images of young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people. This can lead to bullying, blackmail or exploitation.
- The dangers attached to gang culture can rapidly accelerate online as many gangs 'advertise' or promote themselves via websites or social networking sites or if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites, content and images can easily be accessed online (e.g., ignoring age ratings in games enabling exposure to violence, explicit and extreme content; pornography; lifestyle websites such as pro-anorexia, self-harm, suicide or hate sites).
- Young people can be recruited by people with extreme political and cultural views which can lead to their radicalisation.

- Young people becoming the victims of fraud as a result of sharing personal information.

Ignoring the dangers that young people can face would lead to serious gaps in our responsibilities towards safeguarding and child protection. Some of the common technologies used include:

- The Internet
- Email
- Instant messaging
- Blogs / Vlogs
- Podcasts
- Web cameras
- Social networking sites such as Facebook, Twitter and Instagram
- Location based social networking
- Video broadcasting sites such as YouTube
- Chat rooms and forums, Snapchat etc.
- Skype
- WhatsApp
- Online gaming rooms and platforms
- Music download sites
- Mobile phones with camera and video functionality
- Applications (apps)

7. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the college Behaviour Policy.)

Children should have the right to explore the digital environment but also the right to be safe when on it. However, technology often provides the platform that facilitates harm, and the use of technology has become a significant component of many safeguarding issues. Examples of which include child sexual exploitation, child criminal exploitation, radicalisation, sexual predation/grooming, revenge porn and forms of child-on-child abuse such as cyberbullying and nudes and semi-nudes.

In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online, which can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. In accordance with Behaviour in Schools. Advice for Headteachers and school staff (September 2022), the college promotes as part of its culture of excellent standards of behaviour that the same standards of behaviour are expected online as apply offline, and that every student should be treated with kindness, respect and dignity.

An effective approach to online safety empowers a college to protect and educate the whole college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The college will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The issue will also be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support students, as part of safeguarding training (see section 11 for more detail).

The college also sends information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in the college Behaviour Policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the college will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

Staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the college rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of college policy), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the college complaints procedure.

8. Acceptable use of the internet in college

All students, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the college's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the college's terms on acceptable use if relevant.

Use of the college's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Remote Learning

The safeguarding risks associated with virtual and remote learning are similar to those associated with in-person learning. These include peers becoming engaged in inappropriate conversations, using inappropriate or threatening language or abuse, which may encompass behaviour aimed at causing emotional and mental harm/distress.

Examples of different forms of online harm are, online grooming, exposure to harmful content, online sexual harassment and abuse, use of threats or blackmail related to online activity, cyberbullying, online radicalisation, pressure to send sexual image /onward sharing and all variations on these themes. We need to be vigilant and attentive to issues of this matter that can take place online.

It is our responsibility to set the standard of expectations and facilitate positive behaviour for learning online. Education staff need to clearly state high expectations for online communication and behaviour as they would in the physical classroom. Students should be made aware that audio/visual recording of sessions is not acceptable, however it should be stated that all text conversations are recorded automatically.

Before we engage in online video learning sessions, it is important to consider:

Your environment:

- You should locate in a quiet space and inform family members/cohabiters that you are engaging with online learning. This will ensure that the learning environment is focused on the needs of learners and the teacher & student relationship can focus on learning.
- Confidentiality and security need to be maintained and students should feel secure that this is the case.

- You should be dressed appropriately for work and as stipulated in the 'Dress Code' policy. Being dressed in sleep wear or underwear is considered inappropriate and day time clothing must be worn for all online video learning.
- You must choose a 'background' from the selection bar during the video lesson in order to obscure and block students from observing your home area.

The Students Environment:

- Where possible, it is advisable that students are located in a common space in their house, within earshot of parents.
- Students should also use the 'background' function on their computer screens to minimise the ability for others to observe their homes.
- Staff should encourage students to be dressed and ready for learning as if attending college.

9. Students using mobile devices in college

Students may bring mobile devices into college and are handed in at Reception by KS4 Students and returned at the end of the College day, KS5 can have their mobile devices however, these are not permitted to be used during lessons.

Any use of mobile devices in college by pupils must be in line with the acceptable use agreement (see appendices 1 and 2) and our Behaviour Policy.

Any breach of the acceptable use agreement by a pupil may trigger consequences to action in line with the college Behaviour Policy, which may result in the confiscation of their device and further consequences as outlined within the Behaviour Policy.

10. Staff using work devices outside college

Staff members using a work device outside college must not install any unauthorised software on the device and must not use the device in any way which would violate the college's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside college. Any USB devices containing data relating to the college must be encrypted and stored safely.

If staff have any concerns over the security of their device, they must seek advice from the ICT consultants or technician.

Work devices must be used solely for work activities.

11. How the college will respond to issues of misuse

Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the college's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance

with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The college will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the principal and DSL. At every review, the policy will be shared with the governing board.

14.Procedure for managing online safety concerns

Any online safety concerns from staff, students, volunteers or parents must be passed to the Welfare Team immediately as per the Students Safeguarding Procedures. The Welfare Team will then liaise with external agencies where necessary:

- The police where illegal activity is involved (e.g., child sexual abuse images or adult material which breaches legislation).
- Children's Social Care where a referral needs to be made due to a child's vulnerability.
- Adult's Social Care where a referral needs to be made due to an adult's vulnerability.
- the Local Authority Designated Officer (LADO) if the alleged perpetrator is a professional
- parents/carers where appropriate
- Action Fraud- the national fraud and cybercrime reporting centre

Evidence related to the concerns may need to be secured and so equipment may need to be taken temporarily for this purpose.

15. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Anti-Bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENT AND PARENTS/CARERS	
Name of student :	
I will read and follow the rules in the acceptable use agreement policy **When I use the college's ICT systems (like computers) and get onto the internet in college I will:** ● Always use the college's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my username and passwords safe and not share these with others ● Keep my private information safe at all times and not give my name, address, or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ● Always log off or shut down a computer when I'm finished working on it **I will not:** ● Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Log in to the college's network using someone else's details ● Arrange to meet anyone online without first consulting my parent/carer, or without adult supervision **I agree that the college will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (student):	**Date:**
Parent/carer's agreement: I agree that my child can use the college's ICT systems and internet when appropriately supervised by a member of college staff. I agree to the conditions set out above for pupils using the college's ICT systems and internet, and for using personal electronic devices in college, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the college's ICT systems and accessing the internet in college, or outside college on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the college's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the college's network ● Share my password with others or log in to the college's network using someone else's details ● Take photographs of students without checking with teachers first ● Share confidential information about the college, its students or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the college	
I will only use the college's ICT systems and access the internet in college or outside college on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the college will monitor the websites I visit and my use of the college's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside college and keep all data securely stored in accordance with this policy and the college's data protection policy. I will let the designated safeguarding lead (DSL) and ICT technician know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the college's ICT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in college	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the college's acceptable use agreement for staff, volunteers, governors, and visitors?	
Are you familiar with the college's acceptable use agreement for students and parents/carers?	
Do you regularly change your password for accessing the college's ICT systems?	
Are you familiar with the college's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**